

## Claims

- [c1] A method comprising the steps of:
- executing, in a computer system with trusted computing platform capabilities which has an accessible read/write storage device, program instructions effective on powering on of the system to initiate system operation;
  - identifying the presence of the read/write storage device;
  - reading a trusted platform module endorsement public key and storing the public key in a read only area of the read/write storage device;
  - prompting a designated user to enter a password for controlling access to the read/write storage device; and
  - generating a hash value from the password and storing the hash value in a protected area of the read/write storage device for subsequent retrieval in exercising control of system access to the read/write storage device.
- [c2] A method according to Claim 1 executed in a computer system having a hard disk drive as the storage device.
- [c3] A method comprising the steps of:
- executing, in a computer system with trusted computing platform capabilities and which has an accessible read/write storage device, program instructions effective on powering on of the system to initiate system operation;
  - generating in response to powering on of the system a nonce string in the read/write storage device;
  - distinguishing by execution of the program instructions between a requirement for entry of at least one password to access the read/write storage device and no requirement for entry of a password;
  - prompting an operator of the system to enter a password by the execution of the program instructions in response to a determination that entry of a password is required to access the read/write storage device;
  - extending the nonce value and the password to a platform configuration register;
  - quoting the platform configuration register contents to the read/write

storage device;

verifying in the read/write storage device that the quoted contents are derived from the nonce string, the password and the trusted platform module endorsement key; and

granting read/write access to the read/write storage device on verification.

[c4] A method according to Claim 3 executed in a computer system having a hard disk drive as the storage device.

[c5] A method comprising the steps of:

on installation of a read/write storage device in a computer system with trusted computing platform capabilities,

executing, in the computer system receiving the read/write storage device, program instructions effective on powering on of the system to initiate system operation;

identifying the presence of the read/write storage device and storing the TPM endorsement public key in the storage device;

prompting a designated user to enter a password for controlling access to the read/write storage device; and

generating a hash value from the password and storing the hash value in a protected area of the read/write storage device for subsequent retrieval in exercising control of system access to the read/write storage device; then

on subsequent powering on of the computer system;

executing, in the computer system having the read/write storage device, program instructions effective on powering on of the system to initiate system operation;

generating in response to powering on of the system a nonce string in the read/write storage device;

prompting an operator of the system to enter a password by the execution of the program instructions;

extending the nonce string and the password into a platform configuration register;

quoting the platform configuration register contents to the read/write storage device as a value signed with the TPM endorsement key;  
verifying in the read/write storage device that the quoted content is derived from the nonce string, the password and the TPM endorsement key; and  
granting read/write access to the read/write storage device on verification.

[c6] A method according to Claim 5 executed in a computer system having a hard disk drive as the storage device.

[c7] Apparatus comprising:

- a computer system with trusted computing platform capabilities;
- a read/write storage device accessible to the system;
- a TPM endorsement public key stored in said storage device accessibly to said system and identifying said system and said storage device as being specifically linked; and
- program instructions stored accessibly to said system and said storage device and operative when executing on said system and said storage device to:
  - generate in response to powering on of the system a nonce string in the read/write storage device;
  - prompt an operator of the system to enter a password by the execution of the program instructions;
  - generate a value from the nonce string, the password and said endorsement key;
  - supply the value to the read/write storage device;
  - verify in the read/write storage device that the value supplied is derived from the nonce string, the password and the endorsement key; and
  - grant read/write access to the read/write storage device on verification of the value.

[c8] Apparatus according to Claim 7 wherein said storage device is a hard disk drive.

[c9] Apparatus according to Claim 7 wherein said storage device is housed within said computer system.

[c10] Apparatus according to Claim 7 wherein said storage device is housed externally of said computer system.

[c11] Apparatus comprising:

a computer readable media; and  
program instructions stored on said media accessibly to a computer system and effective, when executed on said computer system, to cause the system to:  
respond to powering on of the computer system by;  
executing, in a computer system having an accessible read/write storage device, program instructions effective on powering on of the system to initiate system operation;  
generating in response to powering on of the system a nonce string in the read/write storage device;  
prompting an operator of the system to enter a password by the execution of the program instructions;  
generating a value from the nonce string, the password and an endorsement key for the system;  
supplying the value to the read/write storage device;  
verifying in the read/write storage device that the value is derived from the nonce string, the password and the endorsement key; and  
granting read/write access to the read/write storage device on verification of the value.

[c12]

Apparatus comprising:

a computer readable media; and  
program instructions stored on said media accessibly to a computer system and effective, when executed on said computer system, to cause the system to:  
respond to installation of a read/write storage device in a computer system by,

executing, in the computer system receiving the read/write storage device, program instructions effective on powering on of the system to initiate system operation;

identifying the presence of the read/write storage device and writing to a read only area of the storage device an endorsement public key derived from a trusted platform module of the system;

prompting a designated user to enter a password for controlling access to the read/write storage device; and

generating a hash value from the password and storing the hash value in a protected area of the read/write storage device for subsequent retrieval in exercising control of system access to the read/write storage device;

then causing the system to;

respond to subsequent powering on of the computer system by;

executing, in the computer system having the read/write storage device, program instructions effective on powering on of the system to initiate system operation;

generating in response to powering on of the system a nonce string in the read/write storage device;

prompting an operator of the system to enter a password by the execution of the program instructions;

generating a value from the nonce string, the password and the system endorsement key;

supplying the value to the read/write storage device;

verifying in the read/write storage device that the value is derived from the nonce string, the password and the system endorsement key; and

granting read/write access to the read/write storage device on verification of the value.